International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.812.3

(11/2015)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

E-health multimedia services and applications – Personal health systems

Interoperability design guidelines for personal health systems: WAN interface: Capability exchange certified device class

Recommendation ITU-T H.812.3

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence	H.420–H.429
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Personal health systems	**H.810–H.819**
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.812.3

Interoperability design guidelines for personal health systems: WAN interface: Capability exchange certified device class

Summary

The Continua Design Guidelines (CDG) define a framework of underlying standards and criteria that are required to ensure the interoperability of devices and data used for personal connected health. They also contain design guidelines (DGs) that further clarify the underlying standards or specifications by reducing options or by adding missing features to improve interoperability.

This specification defines the additional design guidelines for the Capability exchange-enabled AHD and WAN device certified device class (CDC). The purpose of the capability exchange is to reduce the amount of information that must be pre-configured on a device in order to obtain plug and play interoperability. Specifically, capability exchange enables application hosting devices (AHDs) to know what types of messages it can send to the WAN device, by identifying its Continua CDCs. Likewise, capability exchange provides a mechanism for the AHD to inform the WAN device of its capabilities, to enable the WAN device to tailor its communication with the AHD. Capability exchange is mandatory for all WAN devices while it is optional for AHDs.

It is assumed that the AHD is pre-provisioned with a URL, or a set of URLs, denoting the service endpoint of one or more WAN devices. The capability exchange process takes place when the AHD first contacts a WAN device. It may also take place intermittently, to update the information received in the first capability exchange. In most cases, the set of Continua CDCs implemented at a WAN device changes slowly, if at all. Therefore, it is expected that the AHD can store the information about WAN capabilities, and optionally, implement a policy for periodically updating that cache. An AHD might identify several WAN devices in this way, and communicate with one or more for different purposes.

The WAN device describes the information about its supported CDCs in a file called "root file". The root file is a special resource that describes the properties of CDCs and how AHD can start information exchange with these CDCs. The root file and other features of the exchange come from an HL7 standard called hData . It not only defines the root file format, but also defines the operations for exchanging root files, using HTTP using GET and POST operations, often referred to as "REST" (for representational state transfer).

Each Continua CDC (in addition to capability exchange) will use the root file to document information relevant to that capability, including the capability name, the information that can be exchanged under the capability and its format, and URLs for REST operations, if supported by that capability. Details are given in the documentation for the respective Continua CDCs.

Recommendation ITU-T H.812.3 is part of the "ITU-T H.810 interoperability design guidelines for personal health systems" subseries, which is outlined in the table below:

Mapping of CDG 2013, ITU-T H.810 and restructured ITU-T H.810-series

Part	Elements	Clauses in the 2013 CDG "Endorphin"	Clauses in ITU-T H.810 (2013)	Restructured H.810-series (2015)
Part 0	System overview	Up to clause 3, plus Annex A and Appendix G	Up to clause 6, plus Annex A and Appendix V	ITU-T H.810 – System overview
Part 1	TAN/ PAN/ LAN	Clauses 4 to 7, Appendices C, D, M	Clauses 7 to 10, Appendices I, II, XI	ITU-T H.811 – TAN-PAN-LAN interface
Part 2	WAN	Clause 8, Appendices H, I, J, K	Clause 11; Appendices VI, VII, VIII, IX	ITU-T H.812 – WAN interface ITU-T H.812.1 – Observation upload ITU-T H.812.2 – Questionnaires ITU-T H.812.3 – Capability exchange ITU-T H.812.4 – Authenticated persistent session
Part 3	HRN	Clause 9, Appendices E, F, L	Clause 12, Appendices III, IV, X	ITU-T H.813 – HRN interface

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T H.812.3	2015-11-29	16	11.1002/1000/12656

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

List of Tables

Page

List of Figures

Page

0 Introduction

The Continua Design Guidelines (CDG) define a framework of underlying standards and criteria that are required to ensure the interoperability of devices and data used for personal connected health. They also contain additional design guidelines that further clarify the underlying standards or specifications by reducing options or by adding missing features to improve interoperability.

These guidelines define the additional design guidelines for the Capability exchange-enabled AHD and WAN device certified device class (CDC). The purpose of the capability exchange is to reduce the amount of information that must be pre-configured on a device in order to obtain plug and play interoperability. Specifically, capability exchange enables application hosting devices (AHDs) to know what types of messages it can send to the WAN device, by identifying its Continua CDCs. Likewise, capability exchange provides a mechanism for the AHD to inform the WAN device of its capabilities, to enable the WAN device to tailor its communication with the AHD. Capability exchange is mandatory for all WAN devices while it is optional for AHDs.

It is assumed that the AHD is pre-provisioned with a URL, or a set of URLs, denoting the service endpoint of one or more WAN devices. The capability exchange process takes place when the AHD first contacts a WAN device. It may also take place intermittently, to update the information received in the first capability exchange. In most cases, the set of Continua CDCs implemented at a WAN device changes slowly, if at all. Therefore, it is expected that the AHD can store the information about WAN capabilities, and optionally, implement a policy for periodically updating that cache. An AHD might identify several WAN devices in this way, and communicate with one or more for different purposes.

The WAN device describes the information about its supported CDCs in a file called "root file". The root file is a special resource that describes the properties of CDCs and how AHD can start information exchange with those CDCs. The root file and other features of the exchange come from an HL7 standard called hData [HL7 V3 HRF] [OMG/hData RESTful Trans]. hData not only defines the root file format, but also defines the operations for exchanging root files, using HTTP using GET and POST operations, often referred to as "REST" (for representational state transfer).

Each Continua CDC (in addition to capability exchange) will use the root file to document information relevant to that capability, including the capability name, the information that can be exchanged under the capability and its format, and URLs for REST operations, if supported by that capability. Details are given in the documentation for the respective Continua CDCs.

This Recommendation is part of the ITU-T H.810 sub-series "H.810 Interoperability design guidelines for personal health systems". See [ITU-T H.810] for more details.

0.1 Organization

This CDC guideline is organized in the following manner.

Clauses 0 to 5: Introduction and terminology – These clauses provide overview information which help in comprehending the remainder of the document.

Clause 6: Use cases – This clause provides motivating examples.

Clause 7: Behavioural model – This clause is an overview of sequences of interactions and summarizes typical iterations, constraints and exceptions.

Clause 8: Implementation guidance – This clause provides an informative description of the implementation of the Capability exchange CDC.

Annex A: Normative guidelines – This clause specifies the normative requirements that must be followed by the Capability exchange CDC.

0.2 CDC guideline releases and versioning

See clause 0.2 of [ITU-T H.810] for release and versioning information.

0.3 What's new

To see what is new in this release of the design guidelines refer to clause 0.3 of [ITU-T H.810].

Recommendation ITU-T H.812.3

Interoperability design guidelines for personal health systems: WAN interface: Capability exchange certified device class

1 Scope

This Recommendation specifies design guidelines for the Capability exchange-enabled AHD and Capability exchange-enabled WAN CDCs. The design guidelines specify the testable requirements that must be implemented by the AHD in order to classify it as a Capability exchange-enabled AHD. The Capability exchange-enabled AHD shall be able to retrieve a root file from the WAN device and be able to validate that the root file conform to the HL7 hData hRF document. In addition, the design guidelines specify testable requirements for a WAN device which details how a Capability exchange-enabled WAN device shall respond to the requests from a Capability exchange-enabled AHD and shall be able to validate that the root document conform to the HL7 hData hRF document.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.810] Recommentation ITU-T H.810 (2015), *Interoperability design guidelines for personal health systems*.

All other referenced documents can be found in clause 2 of [ITU-T H.810].

3 Definitions

This Recommendation uses terms defined in [ITU-T H.810].

4 Abbreviations and acronyms

This Recommendation uses abbreviations and acronyms defined in [ITU-T H.810].

5 Conventions

This Recommendation follows the conventions defined in [ITU-T H.810].

6 Use cases

The use cases below are focused on the needs identified for capability exchange.

6.1 AHD obtains WAN device information

Outpatient Adam Everyman is provided with health measurement devices that interact wirelessly with a smart phone application (the AHD). Adam's health practitioner provides a URL in the form of a QR Code (for example) that can be scanned by the smart phone app during the configuration process, directing the AHD to the disease management organization (DMO), a remote monitoring site. DMO remotely monitors patients at home and collects health information from health measurement devices installed at Adam's home. During configuration, the smart phone app contacts the URL and downloads an XML file (the "root file") containing information about DMO's services. By parsing the root file, the AHD determines the Continua certified device classes supported by the

DMO. In this case, the DMO can receive observation uploads and questionnaires using RESTful HTTP and can participate in authenticated persistent sessions.

6.2 WAN device receives AHD information

Having discovered that the DMO can support authenticated persistent sessions, the smart phone app now wants to inform the DMO that it also has the capability of supporting authenticated persistent sessions. To do so, the AHD must first authenticate with the DMO. After authentication, the AHD may use an HTTP POST operation to send its root file (which is different to the DMO root file) to the DMO, using the designated URL supplied in the DMO's root file. The AHD's root file contains information on the AHD's capabilities, including the fact that the AHD can support authenticated persistent sessions. If the AHD subsequently initiates an authenticated persistent session with the WAN device, the WAN device will use the information in the AHD's root file to send unsolicited commands to the AHD.

7 Behavioural models

The following exchange mechanisms are specified for capability exchange service:

- AHD retrieves the WAN root file from the WAN server;
- the AHD sends its root file to the WAN server.

The following diagram illustrates transactions related to the capability exchange use cases described in clause 6.

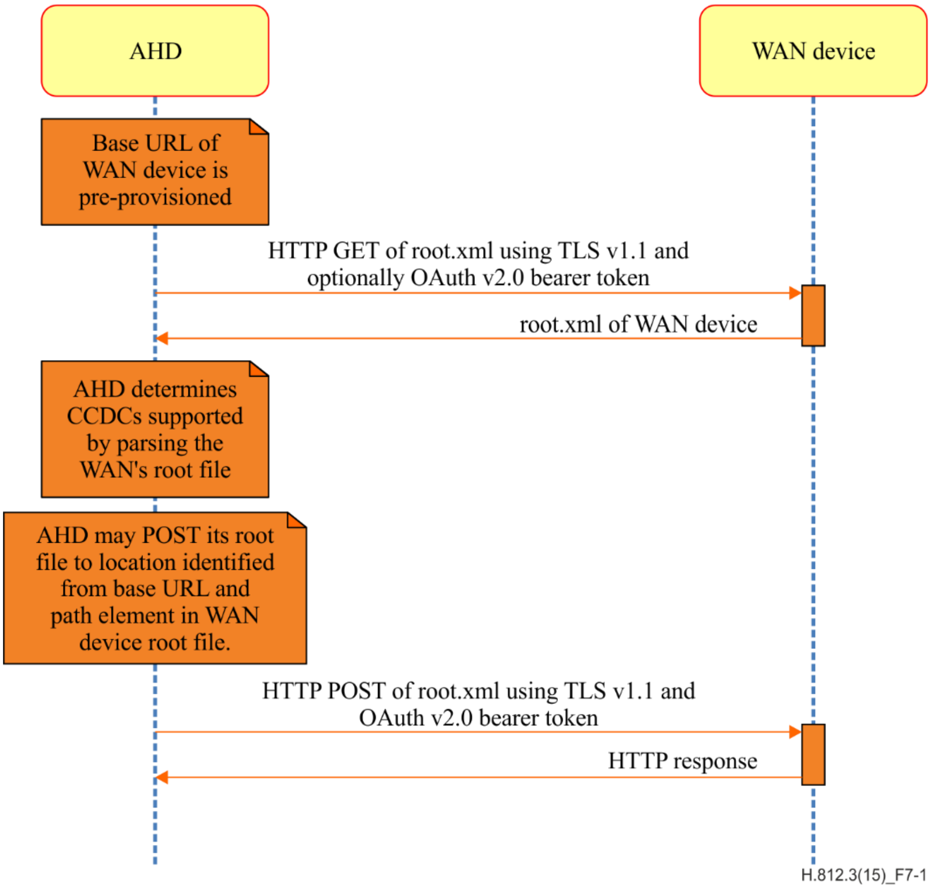

AHD
WAN device
Base URL of WAN device is pre-provisioned
HTTP GET of root.xml using TLS v1.1 and optionally OAuth v2.0 bearer token
root.xml of WAN device
AHD determines CCDCs supported by parsing the WAN's root file
AHD may POST its root file to location identified from base URL and path element in WAN device root file.
HTTP POST of root.xml using TLS v1.1 and OAuth v2.0 bearer token
HTTP response
H.812.3(15)_F7-1

Figure 7-1 – Transactions between AHD and WAN device related to capability exchange

8 Implementation

8.1 Overview

An AHD supporting capability exchange obtains information from the WAN device, and vice versa, in the form of a document called "root". The root file is so named because it exists at the top of the hData hierarchy [HL7 V3 HRF]. The format of the root file is defined in the hData Record Format specification [HL7 V3 HRF]. The WAN must have the capability to provide the root file in XML format, and can optionally provide it in JSON format. Similarly, the AHD must be able to process the root.xml file it receives from the WAN, and optionally, can also process the JSON equivalent.

The root file contains several different types of information useful to the AHD:

– a list of the Continua certified device classes that the WAN device supports,

– a list of the resource types that may be exchanged with the WAN device in one or both directions,

– information about the available representations of exchangeable resources,

– the location of the resources in terms of partial URLs,

– any additional information required by a CCCC listed in the root file.

In the above description, the term "resource" is used in the REST sense: a logical entity that may have multiple representations.

Once the WAN root file has been obtained, the AHD may optionally communicate information back to the WAN device in the form of another root file. The root file sent from the AHD to the WAN device represents the AHD's capabilities, resource types, representations, and other parameters defined by specific CCCCs. This step of sending the AHD root file to the WAN requires authentication, so the WAN can positively identify the AHD that is the source of the root file. The authentication process is not discussed here. Because this step is optional, the AHD root file is not required.

Once capability information has been exchanged, the devices are able to invoke the appropriate protocols in an interoperable fashion. Capability exchange reduces the amount of information that must be pre-configured on a device in order to obtain plug and play interoperability.

8.2 Root file exchange

The root file is exchanged using the following REST mechanism:

– The AHD performs an HTTP GET using a TLS v1.1 secure channel, OAuth v2.0 authorization token of type bearer (use of OAuth is optional in the case where an AHD implements only SOAP based observation upload or consent enabled–AHD CDCs) and a pre-configured URL (the "base URL") to obtain the root.xml file from the WAN device. The AHD is expected to be able to parse the root file and determine the capabilities of the WAN device.

– Optionally, AHD performs an HTTP POST of its root file to the WAN device, using TLS v1.1 secure channel, OAuth v2.0 authorization token of type bearer (use of OAuth is optional in the case where a WAN device implements only SOAP based observation upload or consent enabled –WAN CDCs) and the relative URL indicated by the WAN root file. (The AHD is not assumed to support HTTP server capability, so an HTTP POST is used, rather than a WAN device HTTP GET operation.)

More information about root files and REST methods are available in the hData specifications.

8.3 Contents of the root file

The root file format is described in the HL7 hData Record Format Version 1 Specification [HL7 V3 HRF]. The root files of the WAN and AHD will conform to HRF version 1 and validate with the XSD provided with that specification. In this clause, we profile the elements of the root.xml file. Elements not specifically mentioned in this profile follow the element definitions in the HRF standard. The root file contains the following sub-elements under the top-level <root> element:

– version (xs:integer, 1..1) – The version of the hData Record Format used within the root file. The version number for root files complying with this version of the specification is 1.

– profile (0..*) – This element represents a CCCC supported by the WAN or AHD that owns the root file. Each CCCC is described by one <profile> element using the following sub-elements:

  o id (xs:string, 1..1) – The id is the formal name of the CCCC represented by the profile element. For capability exchange, the formal name is "CapabilityExchange". For other device classes, the version-specific formal name will be given in the Continua documentation for that CCCC.
  o reference(xs:string, 1..1) – A version-specific URL reference to the Continua documentation for the CCCC represented by this profile element. For capability exchange, the reference (which refers to this Recommendation) is " http://handle.itu.int/11.1002/3000/hData/CX/2015/01/CapabilityExchange.xsd".

– resourceType (1..*) – This element represents a resource type associated with one or more of the profiles listed in the root file. A specific resource type can be used in one or more CCCC. A resource type is represented by the following sub-elements:

  o id (xs:string,1..1) – This attribute contains the name for the resourceType. For capability exchange, the only resourceType is "root". For other CCCCS, the resource id(s) are given in the CCCC documentation.

  o reference(xs:string, 1..1) – A version-specific reference to the semantic definition of the resource type. For the root resource type used by capability exchange, the reference is "http://www.hl7.org/implement/standards/product_brief.cfm?product_id=261".

  o representation (0..*) – This element represents each serialization format of the resource available for "on the wire" communication.

    ▪ mediaType (xs:string, 1..1) – Contains the media type of the resource. For capability exchange, the required media type is "application/xml". An optional second representation is "application/json".

    ▪ validator(xs:string, 0..*) – An optional reference to a validator for this representation, such as an XML schema definition (XSD) or Schematron.

– section (1..*) – A section represents a "virtual file folder" where instances of a certain resource type are found. A section is identified by partial URL, relative to the base URL. Each CCCC may define one or more sections. For capability exchange, there is one required section in the WAN root file.

  o path (xs:string, 1..1) – This text attribute is a path segment, used to construct the full path to the section. For capability exchange, the path is "roots".

  o profileID(xs:string, 0..*) – The <id> of the CCCC defining this section. The value of this element MUST be equal to the id attribute of a <profile> element.

  o resourcePrefix(xs:boolean, 0..1) – This element is omitted.

- resourceTypeID (xs:string, 0..1) – The value of this element MUST be equal to the id attribute of a <resourceType> element. Only resources whose type matches the resourceTypeID element can appear in the section. If no resourceTypeID is given, the section may not contain resources, only other sections.
- metadataSupport(xs:boolean, 0..1) – This element is omitted.
- section (section, 0..*) – The subsections belonging to the current section, if any.

In addition to these elements, each CDC may define extensions to the root file. The required extension elements, if any, will be present when the corresponding CDC is declared in the <profile> element.

8.4 Optional JSON version of root file

The WAN may optionally support a JSON version of the root.xml file. If the AHD requests "application/json" in the HTTP accept header, and the WAN supports the JSON, the WAN should return the JSON version of the root file.

The JSON version of the root file contains the same information as the XML version. The transform from XML to JSON and the JSON root file format is discussed in [HL7 V3 HRF].

Annex A

Normative guidelines

(This annex forms an integral part of this Recommendation.)

Table A.1 – Normative guidelines for WAN devices

Name	Description	Comments
CapX_WAN_Root_ Standard	Root file of the WAN device shall comply with [HL7 V3 HRF].	
CapX_WAN_Root_ Security	WAN device shall support TLS v1.1 as defined in [ITU-T H.812]. All hData based WAN devices shall support OAuth authorization token of type bearer as defined in [ITU-T H.812].	A WAN device that implements only SOAP based observation upload or consent enabled-WAN CDCs is not required to support the Capability Exchange-WAN CDC.
CapX_WAN_Root_Profile	The root file of the WAN device shall contain a profile element for each CDC it supports.	
CapX_WAN_Root_XML_ Version	The WAN device shall support an XML version of its root file.	
CapX_WAN_Root_JSON_ Version	The WAN device may support a JSON version of its root file.	Note that the HL7 hRF specification document does not specify schema for validating JSON formatted root file.
CapX_WAN_Root_ Validation	The XML root file of the WAN shall validate against the hData Version 1 root.xsd	
CapX_WAN_Root_CDC_ Conformance	A WAN device listing a particular CDC in its root file shall conform to the normative guidelines for that CDC.	
CapX_WAN_Root_ Version	The version number in the WAN root file conforming to this specification shall be 1	
CapX_WAN_Root_ Profile_Element	The Health & Fitness Service root file **shall** contain a profile element with the id "CapabilityExchange" and reference "*http://www.continuaalliance.org/products/design-guidelines H.812.3 Capability Exchange*"	
CapX_WAN_Root_ ResourceType_Element	The WAN root file shall contain a resourceType with id "root" and reference "http://www.hl7.org/implement/standards/product_brief.cfm?product_id=261"	

Table A.1 – Normative guidelines for WAN devices

Name	Description	Comments
CapX_WAN_Root_ MediaType_XML	The WAN root file shall have a representation element under the "root" resourceType with mediaType "application/xml".	
CapX_WAN_Root_ MediaType_JSON	The WAN root file may have a representation element under the "root" resourceType with mediaType "application/json"	
CapX_WAN_Root_ Section_Element_ Inclusions	The WAN root file shall have a section element with the path "roots", the profileID "CapabilityExchange", the resourceTypeID of "root", and shall not specify the resourcePrefix or metadataSupport elements.	
CapX_WAN_Root_ Section_Element_ Exclusions	The WAN root file section element with the path "roots" shall not specify the resourcePrefix or metadataSupport elements.	
CapX_WAN_REST_ Standard	The WAN responses to HTTP method calls shall comply to OMG hData REST Binding for RLUS [OMG/hData RESTful Trans].	
CapX_WAN_REST_GET_ XML_Response	By default, the WAN device shall respond to a root file GET request (i.e., an HTTP GET on [baseURL]/root) by returning the XML version of the WAN's root file.	
CapX_WAN_REST_GET_ JSON_Response	A WAN device which has an "application/json" representation element under the "root" resource type in its root file shall return the JSON version of its root file in response to a AHD's GET request that specifies "application/json" in the HTTP accept header. If the WAN device does not have the JSON version then it shall return HTTP status code 501 Not Implemented.	
CapX_WAN_REST_ POST_Response	The WAN device shall accept a HTTP POST at the URL [baseURL]/roots only if the sending AHD has a valid authorization token of type bearer as defined in [ITU-T H.812].	
CapX_WAN_REST_ POST_Unauthenticated_ Sender	If any content is posted to the WAN device by an unauthorized sender, then the WAN device shall respond with a HTTP 401 Unauthorized error.	

Table A.1 – Normative guidelines for WAN devices

Name	Description	Comments
CapX_WAN_REST_ POST_XML_Validation	When an XML file is POSTed to the URL [baseURL]/roots, the WAN device shall validate the file against the hData Version 1 root.xsd and return HTTP 201 if the file is validated, and in case of validation failure, return HTTP 422 Unprocessable Entity.	
CapX_WAN_REST_ POST_JSON_Validation	When a JSON file is POSTed to the URL [baseURL]/roots, the WAN device shall return HTTP 422 Unprocessable Entity if the JSON does not conform to the hData root file specification and otherwise return HTTP 201.	Note that the HL7 hRF specification document does not specify schema for validating JSON formatted root file.
CapX_WAN_REST_ POST_Response	In response to a successful POST of the AHD root file to [baseURL]/roots, the WAN device shall return the unique URL of the newly-created root resource.	

Table A-2 – Normative guidelines for AHD device

Name	Description	Comments
CapX_AHD_REST_ XML_Request	Given the URL of a WAN device complying with capability exchange ("baseURL"), the AHD device may obtain the root file of the WAN device using an HTTP GET operation.	
CapX_AHD_REST_ WAN_Root_security	AHD shall obtain root file of the WAN device using TLS v1.1 secure channel as defined in [ITU-T H.812]. All hData based AHDs shall support OAuth authorization token of type bearer as defined in [ITU-T H.812].	An AHD that implements only SOAP based observation upload or consent enabled-AHD CDCs is not required to support the Capability Exchange-AHD CDC.
CapX_AHD_REST_ XML_Request	The AHD device shall be able to request the WAN root file in XML format by specifying "application/xml" in the HTTP accept header.	
CapX_AHD_REST_ JSON_Request	The AHD device may request the WAN root file in JSON format by specifying "application/JSON" in the HTTP accept header.	Note that the HL7 hRF specification document does not specify schema for validating JSON formatted root file.
CapX_AHD_Root_POST	AHD may do an HTTP POST of its root file at the URL [baseURL]/roots using TLS v1.1 secure channel as defined in [ITU-T H.812] and a valid authorization token of the type bearer as defined in [ITU-T H.812]. The authorization token shall be obtained according to the guidelines described in [ITU-T H.812].	
CapX_AHD_Root_ Standards	Root file of the AHD shall comply with [HL7 V3 HRF].	
CapX_AHD_Root_Profile	The root file of the WAN device shall contain a profile element for each CDC it supports.	
CapX_WAN_Root_CDC_ Conformance	An AHD listing a particular CDC in its root file shall conform to the normative guidelines for that CDC.	For example profile and section info in the root file for a CDC are defined by that specific CDC.

Appendix I

Root file inclusions for capability exchange

(This appendix does not form an integral part of this Recomemndation.)

I.1 Required root file inclusions for WAN device

```
<profile>
  <id> CapabilityExchange</id>
  <reference>http://www.continuaalliance.org/products/design-guidelines  H.812.3
Capability Exchange
  </reference>
</profile>

<section>
 <path>roots</path>
 <profileID> CapabilityExchange</profileID>
 <resourceTypeID>root</resourceTypeID>
</section>

<resourceType>
 <id>root</id>
 <reference>
http://www.hl7.org/implement/standards/product_brief.cfm?product_id=261
   </reference>
 <representation>
     <mediaType>application/xml</mediaType>
 </representation>
 <representation> <!-- optional -->
     <mediaType>application/json</mediaType>
 </representation>
</resourceType>
```

I.2 Schema for the root.xml

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
targetNamespace="http://hl7.org/schemas/hdata/2013/08/hrf"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:hrf="http://hl7.org/schemas/hdata/2013/08/hrf">
 <xs:element type="xs:string" name="id"/>
 <xs:element type="xs:float" name="version"/>
 <xs:element type="xs:dateTime" name="created"/>
 <xs:element type="xs:dateTime" name="lastModified"/>
 <xs:element type="xs:string" name="name"/>
 <xs:element type="xs:anyURI" name="uri"/>
 <xs:element type="xs:string" name="email"/>
 <xs:element type="xs:string" name="reference"/>
 <xs:element type="xs:string" name="path"/>
 <xs:element type="xs:string" name="profileID"/>
 <xs:element type="xs:boolean" name="resourcePrefix"/>
 <xs:element type="xs:string" name="resourceTypeID"/>
 <xs:element type="xs:boolean" name="metadataSupport"/>
 <xs:element type="xs:string" name="mediaType"/>
 <xs:element type="xs:string" name="validator"/>
 <xs:group name="extensionElement">
  <xs:sequence>
   <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
   <xs:any namespace="##local" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
 </xs:group>

 <xs:element name="author">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="hrf:name"/>
    <xs:element ref="hrf:uri" minOccurs="0"/>
    <xs:element ref="hrf:email" minOccurs="0"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>

 <xs:element name="profile">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="hrf:id"/>
    <xs:element ref="hrf:reference"/>
    <xs:group ref="hrf:extensionElement" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>

 <xs:element name="section">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="hrf:path"/>
    <xs:element ref="hrf:profileID" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element ref="hrf:resourcePrefix" minOccurs="0"/>
    <xs:element ref="hrf:resourceTypeID" minOccurs="0"/>
    <xs:element ref="hrf:metadataSupport" minOccurs="0"/>
    <xs:group ref="hrf:extensionElement" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element ref="hrf:section" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>

 <xs:element name="representation">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="hrf:mediaType"/>
    <xs:element ref="hrf:validator" minOccurs="0" maxOccurs="unbounded"/>
    <xs:group ref="hrf:extensionElement" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>

 <xs:element name="resourceType">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="hrf:id"/>
    <xs:element ref="hrf:reference"/>
    <xs:element ref="hrf:representation" minOccurs="0" maxOccurs="unbounded"/>
    <xs:group ref="hrf:extensionElement" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="root">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="hrf:id"/>
    <xs:element ref="hrf:version"/>
    <xs:element ref="hrf:created"/>
    <xs:element ref="hrf:lastModified"/>
    <xs:element ref="hrf:profile" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element ref="hrf:section" maxOccurs="unbounded"/>
    <xs:element ref="hrf:resourceType" minOccurs="0" maxOccurs="unbounded"/>
    <xs:group ref="hrf:extensionElement" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
  </xs:complexType>
  <xs:key name="PKResourceType">
   <xs:selector xpath="hrf:resourceType/hrf:id"/>
   <xs:field xpath="."/>
  </xs:key>
  <xs:keyref name="FKSectionToResourceType" refer="hrf:PKResourceType">
   <xs:selector xpath="hrf:section/hrf:resourceTypeID"/>
   <xs:field xpath="."/>
  </xs:keyref>
  <xs:key name="PKProfile">
   <xs:selector xpath="hrf:profile/hrf:id"/>
   <xs:field xpath="."/>
  </xs:key>
  <xs:keyref name="FKSectionToProfile" refer="hrf:PKProfile">
   <xs:selector xpath="hrf:section/hrf:profileID"/>
   <xs:field xpath="."/>
  </xs:keyref>
 </xs:element>
</xs:schema>
```

I.3 Required root file inclusions for AHD

No required inclusions, however an AHD device listing a particular CDC in its root file (as a profile element) **shall** conform to the normative guidelines for that CDC.

Appendix II

hData

(This appendix does not form an integral part of this Recomemndation.)

hData is a lightweight, web-based specification for exchanging electronic health data. Created in 2009 by US non-profit MITRE Corporation and evolved in cooperation with leaders in the health care industry, hData is the first RESTful standard for health data exchange. The hData specifications have been approved by Health Layer 7 (HL7) and the Object Management Group (OMG).

hData uses REST (Representational State Transfer) over HTTP in a way that separates content, transport and security. REST is a design pattern that is simple, scalable and widely adopted.

hData is used in all Continua device classes, either as the only mechanism, or as an alternative to SOAP based exchange.

Resources are a central concept in REST and in hData. A resource can be any piece of information: data about a patient, a device, a prescription, a plan of care, an imaging study, a problem or condition, or a complete medical document such as a Consolidated CDA [HL7 CDA IHE HSC]. For purposes of information exchange, resources can have multiple representations, such as XML or JSON.

Sections represent a virtual arrangement of resources in hData. Sections are analogous to directories in a hierarchical file system, and are defined by paths consisting of one or more forward-slash delimited sub-levels. Each section is associated with a specific type of resource (called *resourceTypes* in hData). For example, resources that represent a person's allergies may be found in a section called *allergy*. The allergy section may contain zero or more instances of an allergy resource. The arrangement of sections forms a tree structure, called the hData Hierarchy (HDH).

URLs uniquely identify each resource. The URL of a resource is a combination of a base URL, a section path, and a resource ID, as follows:

```
    resource URL = (baseURL)/(sectionPath)/(resourceID)
```

The baseURL is the location of the hData service endpoint, and consists of the protocol (in this case, HTTP or HTTPS), a host identifier (IP address or domain name), and optionally a port. The resourceID is defined arbitrarily by the resource owner, subject to the constraint that the resource URL is unique.

Root Files are provided by hData service endpoints to advertise the resource types (extensions) and the section paths (sections) provided by that service. The format of the root file is described in [HL7 V3 HRF]. The root file is accessed by a HTTP GET operation on the following URL:

```
    root file URL = (baseURL)/root
```

Content Profiles are the means to achieve interoperability between hData service endpoints. Content profiles are implementation guides that describe an application of hData that promote information interoperability. If every hData service endpoint were to arbitrarily define its own resource types and hData hierarchy, the result would be an ecosystem with no predictability or consistency, with naming conflicts and incompatible resource schemas. To counteract this potentially chaotic situation, hData calls for the creation of content profiles which provide standard section naming and resource schemas for a specific business need or technical capability. For example, pharmacy domain experts have provided a Content Profile for Medication Statements [b-

HL7 V3IG MSSP]. Conforming to this content profile assures interoperability of medication statements among providers and consumers of this type of information.

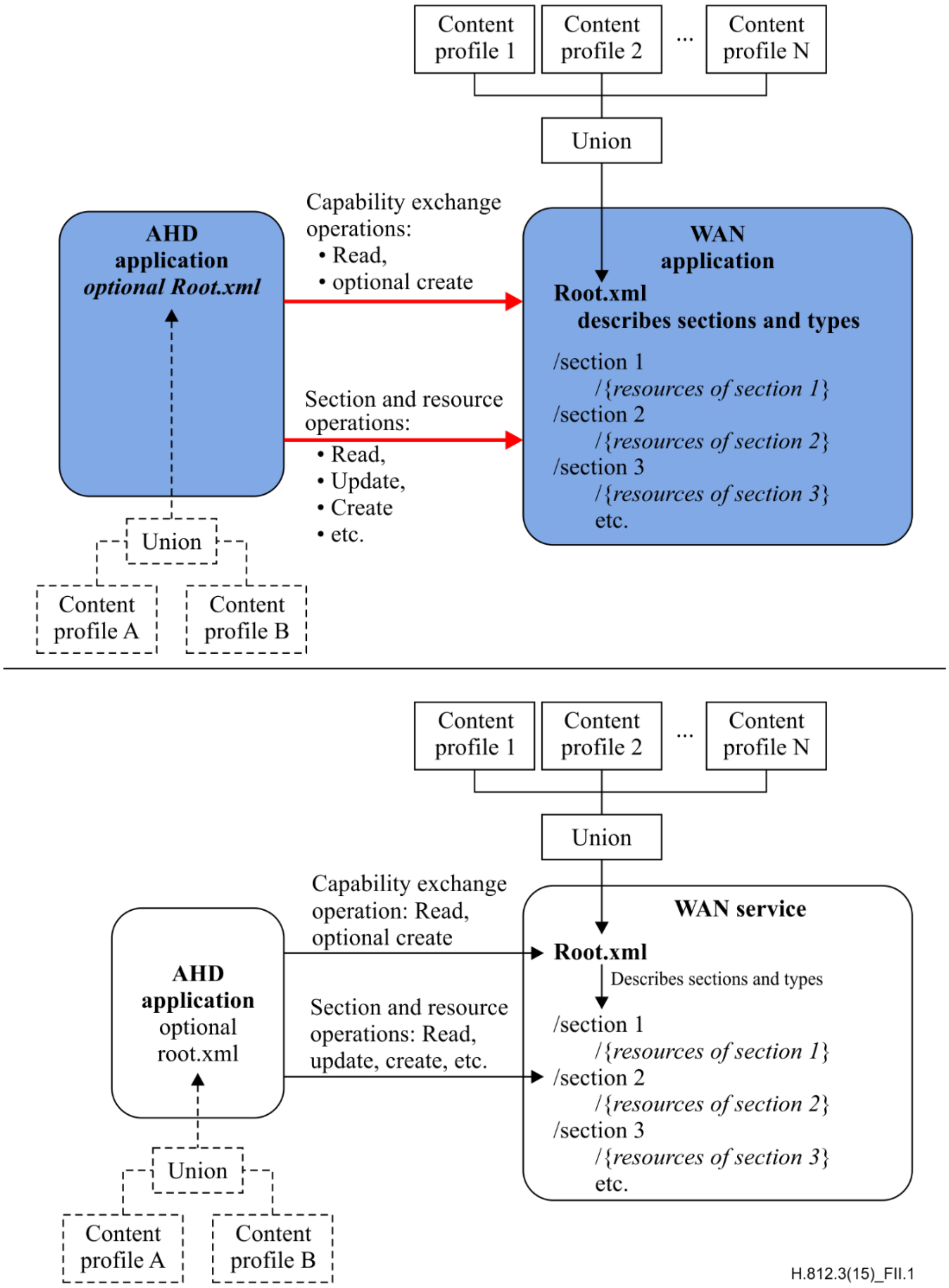
Each certified device class (CDC) defines one or more resource types and associated section paths in an hData content profile. If an hData service endpoint supports more than one CDC, then its root file will effectively be a union of those extensions and section paths. To create a root file from multiple HCPs, the implementer should copy and combine the information in the example root files from each HCP to create a single root file, creating a combined list of profiles, sections, and resourceTypes. The result is an HDH that combines multiple CDCs.

REST Operations, summarized in Table II.1, are at the heart of hData. There are three types of operations: resource operations, section operations, and base operations, corresponding to the target being a resource (baseURL/sectionPath/resourceID), a section (baseURL/sectionPath), or the base (baseURL), respectively. hData represents a REST binding of a Retrieve, Location and Updating Service (RLUS). For details, including information on required and optional behaviours and parameters, and return arguments, see [OMG/hData RESTful Trans] the hData RESTful transport specification.

Table II.1 – Types of operations

Operation	Operation description	HTTP implementation	Requirement
Read	Get the current version of the resource	GET (*resourceURL)*	Required
Version Read	Get a specific version of the resource	GET (*resourceURL*)/history/(*versionId*)	Optional
Update	Update an existing resource	PUT *(resourceURL)*	Optional
Delete	Delete a resource	DELETE *(resourceURL)*	Optional
List	Gets a list of subsections and resources in the section as an ATOM feed	GET (*baseURL or sectionURL*)	Required
Create	Create a new resource or subsection in a section	POST (*baseURL or sectionURL*)	Optional
Batch Create/ Update	Create or update multiple resources in a section	POST (*baseURL or sectionURL*) using Atom feed	Optional
Search	Gets a list of section resources matching the query parameters	GET *(baseURL or sectionURL)/* ?search*(queryString)*	Optional
Validate	Validate a proposed creation action, prior to commit	POST (*sectionURL*)/validate	Optional
Capability Read	Gets root file for capability exchange	GET (*baseURL*)/root	Required
Metadata	Gets service metadata; returns security mechanisms available and a list of supported hData content profiles	GET (*baseURL*)/metadata, optionally OPTIONS (*baseURL*)	Required without prior authentication or authorization
Update Metadata	Replaces metadata on document	POST (*resourceURL)*	Optional

The hData interoperability framework is depicted in Figure II.1.



Content profile 1
Content profile 2
...
Content profile N
Union
AHD application optional Root.xml
Capability exchange operations:
• Read,
• optional create
WAN application
Root.xml describes sections and types
/section 1
/{resources of section 1}
/section 2
/{resources of section 2}
/section 3
/{resources of section 3}
etc.
Section and resource operations:
• Read,
• Update,
• Create
• etc.
Union
Content profile A
Content profile B
Content profile 1
Content profile 2
...
Content profile N
Union
Capability exchange operation: Read, optional create
WAN service
Root.xml
Describes sections and types
AHD application optional root.xml
Section and resource operations: Read, update, create, etc.
/section 1
/{resources of section 1}
/section 2
/{resources of section 2}
/section 3
/{resources of section 3}
etc.
Union
Content profile A
Content profile B
H.812.3(15)_FII.1

Figure II.1 – hData interoperability framework

(NOTE – The AHD application and WAN application root.xml files are **not** the same.)

Bibliography

All referenced bibliography entries can be found in [ITU-T H.810].

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016